



NETCOM / 9th Army Signal Command



Active Directory (AD) Summit

Army Active Directory Status and Implementation Guidelines

Robert Bachert

Robert.bachert@us.army.mil

520-533-1855

MAJ Earl Robinson

(703) 806-0755

Earl.robinson@us.army.mil



Agenda

- Purpose
- Overview
- AD Guidelines
- AD Army-Wide
- Implementation/Migration Planning
- Road Ahead



Purpose

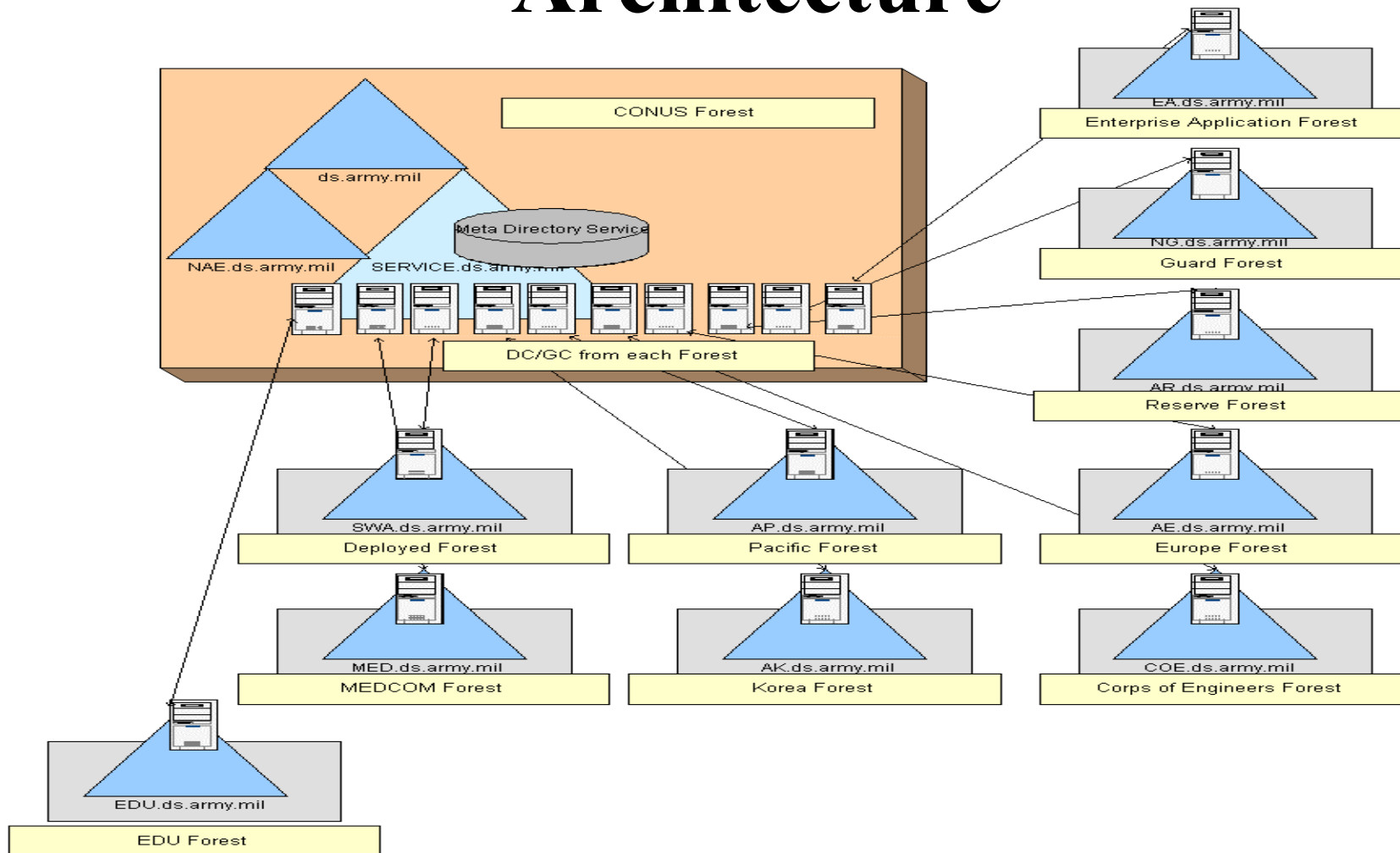
- Provide an Active Directory status and emerging guidelines for planning and implementation Army Wide.
- To provide organization and installations Active Directory Project Officers, an update to the PM's FY 04 Active Directory Implementation Plan..



NETCOM / 9th Army Signal Command



Army Active Directory Forest Architecture





Guidelines: Why AD?

- Microsoft support for NT 4.0 server ends Dec 04
- Army is currently ~95% NT 4.0
- Once Microsoft support ends, the Army is at risk
 - IAVA patches (requires separate support contract with Microsoft)
 - Reduced use of COTS software as commercial vendors stop producing software for the NT 4.0 environment
- Current NT 4.0 LAN-based architecture will not support the Objective Force/Net-centric Force
 - Highly segmented, isolated islands focused on local needs and security
 - Limited levels of trust and interoperability between domains
 - Labor intensive operations to support cross-LAN access
 - No ability to create a global Army directory of users and resources available for shared mission support
- All future Microsoft Operating Systems are AD enabled



NT 4.0 Technology Replacement

NT member servers & User client OS's can Be replaced with Windows 2000 or better however some applications may not operate with Win2K OS

Must be upgraded to AD to provide Network OS

NT Network Domain

Controllers

Network based upon Domain Controller OS

NT Member Servers

Print, file, application c.

... Clients can be upgraded to Win 2K but if NT domain controllers Server OS's are replaced With Windows 2000 or better, The network is an Active Directory network

Exchange 5.5 operate as member server with Win2K OS within either NT 4.0 or AD Network environment.

(Researching)

User Clients

Exchange 5.5

E-Mail

Conclusion:

A decision to get off of NT Is a decision to implement Active Directory.



AD Guidance's

- Preliminary Guidance for Deploying Microsoft Windows 2000, Dated 14 Feb 2000
- Draft Active Directory Policy for Forest/Domain Approval Process
- Army G3 Workstation Guidance on 9X clients
- AD Implementation Technical Guidance Package
- NETCOM TECHCOM Implementation Memorandums



AD Guidelines Sources

- AD Summits
 - Implementation Of AD in the Army
- AD Implementation Technical Guidance Package
 - Consists of eleven documents that
 - Provide customers guidance to get ready for AD and to implement an AD forest/domain or a top-level OU
 - Provide an organization with the required technical guidance needed to implement AD within the Army Enterprise Infostructure (AEI) environment.
- Master Configuration Cookbook
- Lessons learned (MDW, MEDCOM, AF and other DoD Agencies)



Guidelines: Role of AD

- Support LAN Client/Server operations (e.g., user authentication, printing, and sharing of files)
- Support the Single DOIM Concept (Administration Delegation)
- Support installation-level Exchange e-mail
 - Upgrade Exchange OS to Windows 2000
 - Decouple Exchange migration, target Exchange 2003
- Support Server Consolidation
- Standard Domain Controller Configuration
- Support Windows Server 2003 as the target Operating System (OS)
- Decouple from Army wide implementation of standard desktop OS



Role Of AD (Continued)

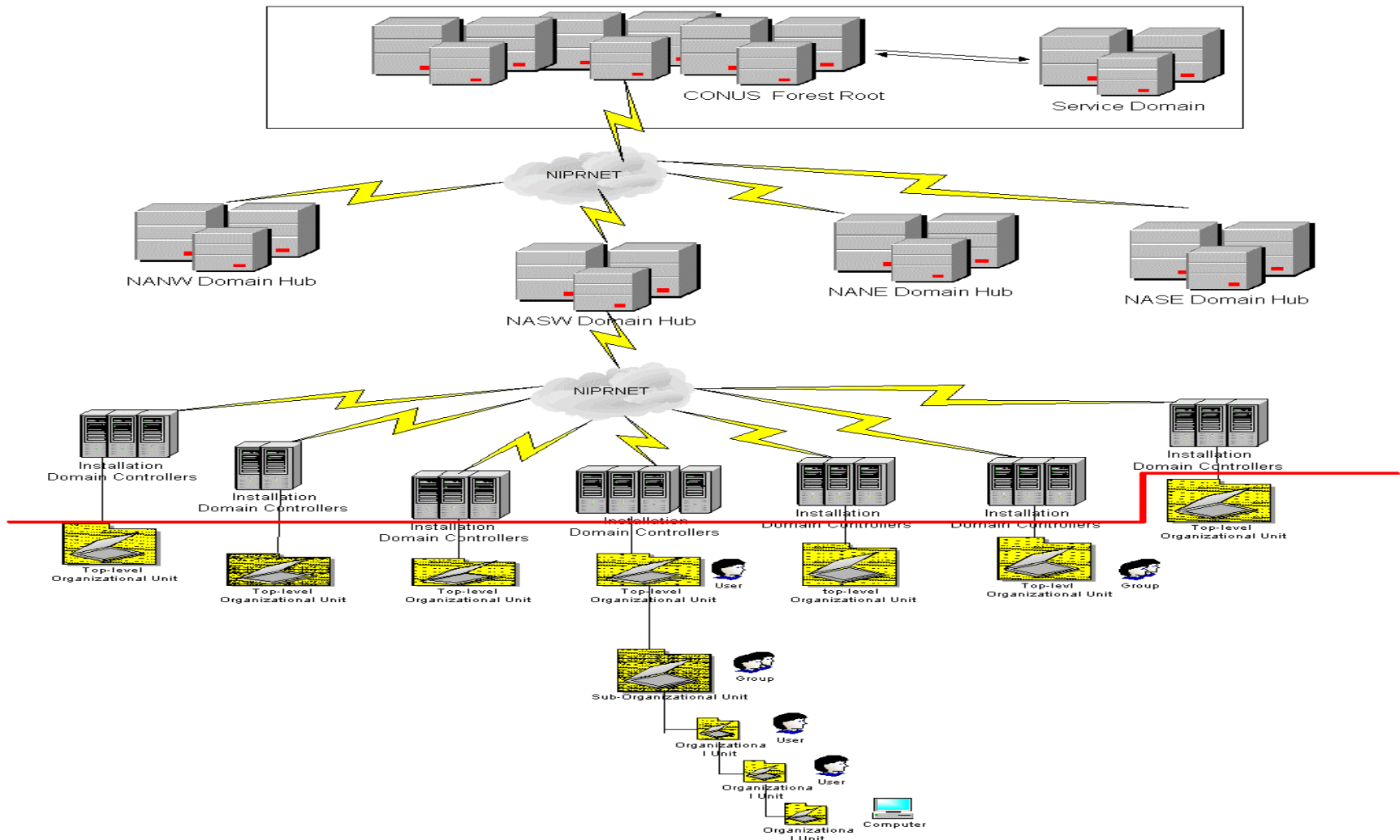
- Provide central control of AD Naming Convention and Schema and strict physical security / administration of AD Domain Controllers
- Secure AD sensitive traffic using IPSec between DC to DC Over WAN
- Microsoft Certificate Authority Design
- Integration of AD into the Horse blanket



NETCOM / 9th Army Signal Command



Army AD Forest Design





Army AD Implementation

- TNOSC manages regional domains using enterprise tools licensed for site support (domain controllers/critical servers)
- Site/installation support is migrated into an appropriate Organizational Unit (OU)
- OU structure operated under the Single DOIM Concept based on admin capabilities delegated from the TNOSC DOIM
- Site implementation/migration plan may further delegate selected responsibilities to IMOs
- Domain Controllers in DOIM Facilities



Implementation Strategy

- PM DCACS/PM BES is the AD Implementer
- Centralized management with decentralized execution
 - AD Backbone centralized funding.
 - Centralized procurement of AD servers and software using core funds (Standard Configuration)
 - Limited centralized funding for site implementation
 - NETCOM approves Site Specific Implementation Plan (SSIP)
- Site Develops SSIP
 - Network Diagram
 - Migration plan
 - OU Structure
 - Resource Plan
- Four Phase Implementation Approach



AD Four Phase Implementation

Pre-migration

Pre-Planning

- Surveys
- SSIP
- Templates

Phase 1

- “AD Forest and Hubs”

PM/PCO
& TNOSC

- Establish Root
- Establish Regional Hubs
- Review and approve SSIP

Phase 2

- Extend AD to Sites

PM/PCO
& TNOSC

- Establish Installation DCs
- Populate Top-level OU

Phase 3 & 4:

- Implement SSIP
- Post-Migration Actions

PM/PCO
& DOIM

PM/PCO
& DOIM

- Implement SSIP
- Migrate Computer accounts & users
- Post Migration
- Clean-up
- QA

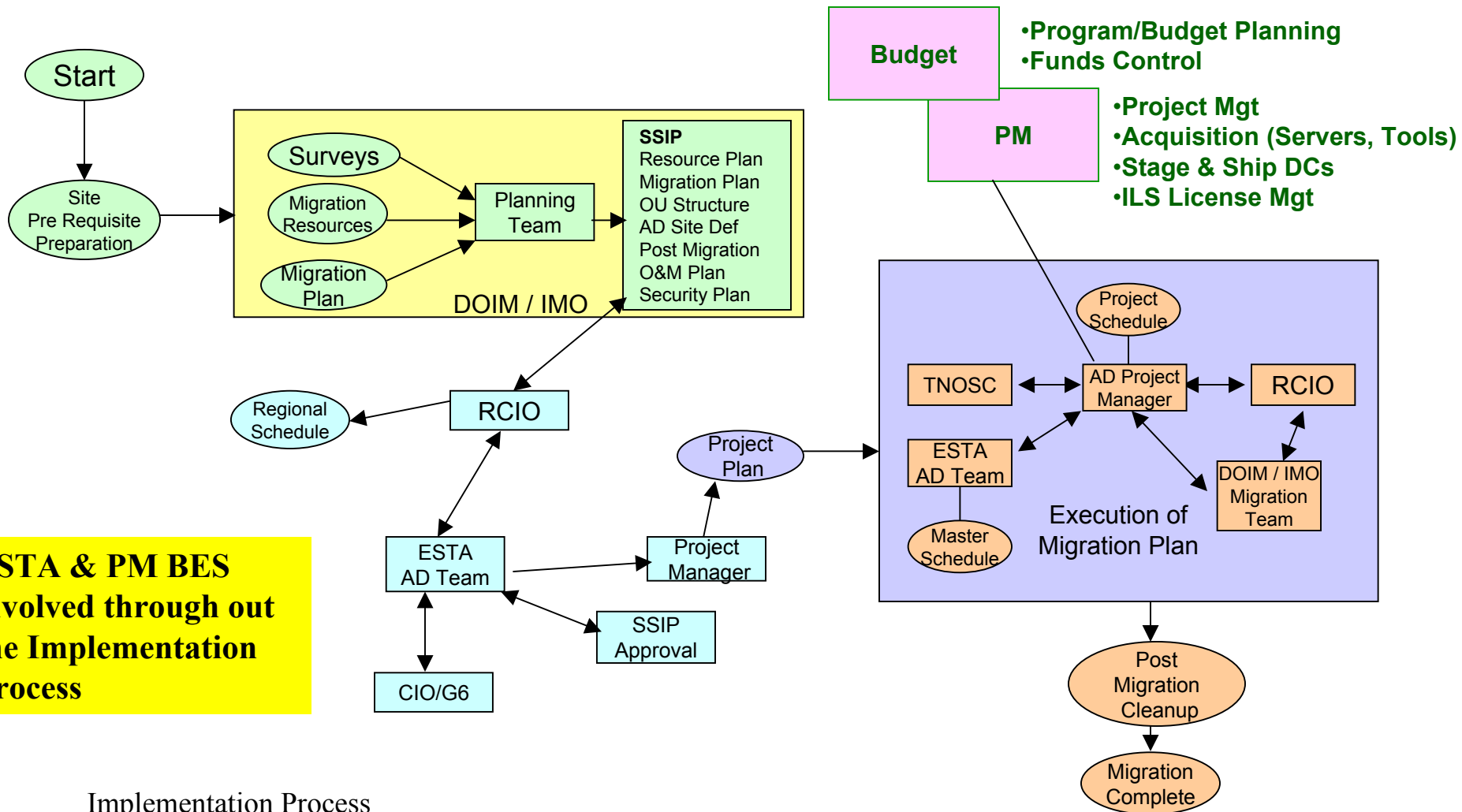
- Configure DCs
- Acquire H/W & S/W
- Approve SSIP
- Seek Funds

- Templates
- Project Mgt Support
- Tech Support

NETCOM with PM Support provides overall guidance and technical support during all phases



Planning & Implementation Process





AD Implementation Cost

- NETCOM is working with the CIO/G6 & PM BES to core fund the cost of O&M of all domain controllers.
- NETCOM will work with IMAs and RCIOs to identify and program for the cost of the AD Migration.
- Need to develop an approach that addresses funding reallocation to resource the O&M of AD Site operations.



Road Ahead

- Develop Forest and Regional Schedule for AD migration
- Prepare Servers and Desktops for AD Aware
- NETCOM & PM BES Work together on
 - Develop an Army-Wide AD Implementation Schedule
 - Emerging security guidelines
 - Funding requirement for TNOSC support
 - Review of implementation plans
 - Site support
 - Developing a Master Migration Schedule
- Work Funding Issues





Issues

- The Use of Windows 2003 encryption Module (Dec 2003)
- Site Migration Resources
- Exchange 5.5



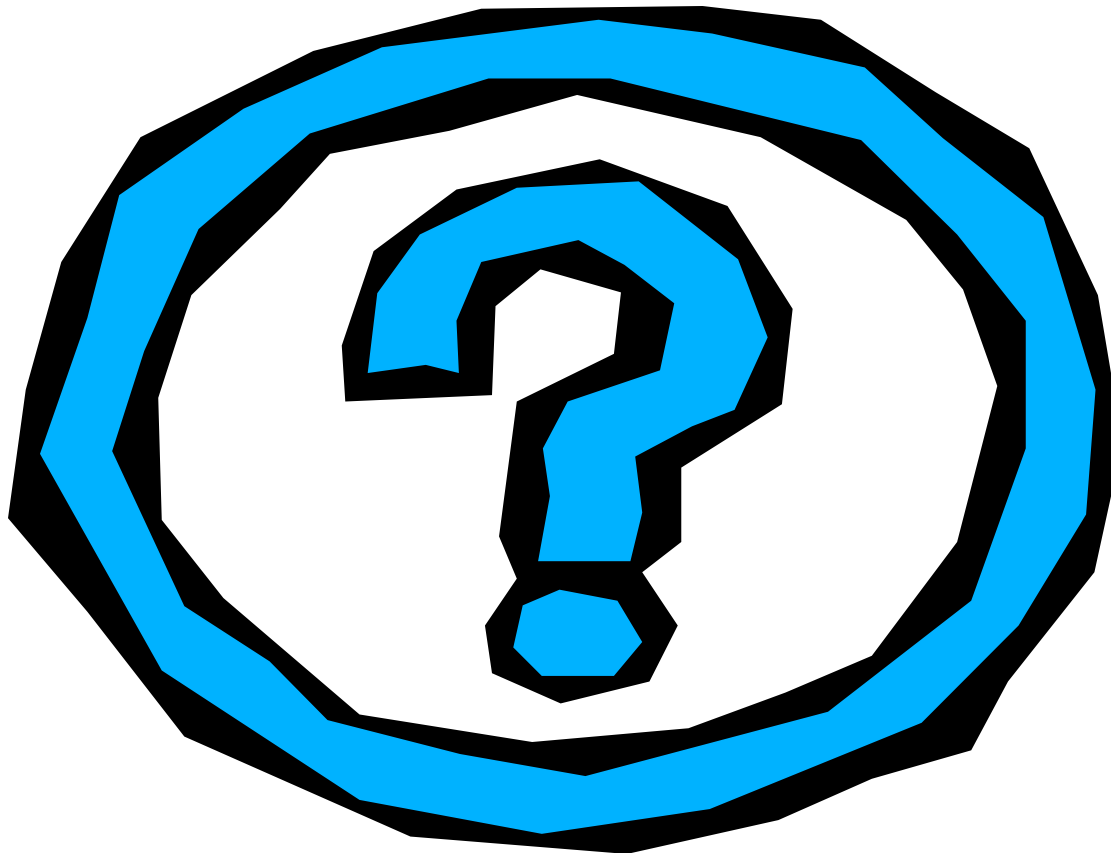
NETCOM & PM Milestones

- Oct Sites start initial preparation for implementation
- Oct-Nov PM BES Conduct Site Surveys
- Nov AD Summit AD Readiness (NETCOM, PM BES)
- Dec Stand up CA (Root, Forest and Domain)
- Dec Transition CONUS Root to Win2003 OS
- Dec Start Implementation of AD Backbone
- Jan Start Site Migrations





NETCOM / 9th Army Signal Command



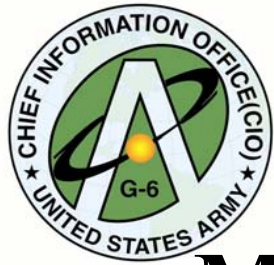
Robert.Bachert@us.army.mil
Bobby.Smith@us.army.mil



NETCOM / 9th Army Signal Command



Back-UP Slides

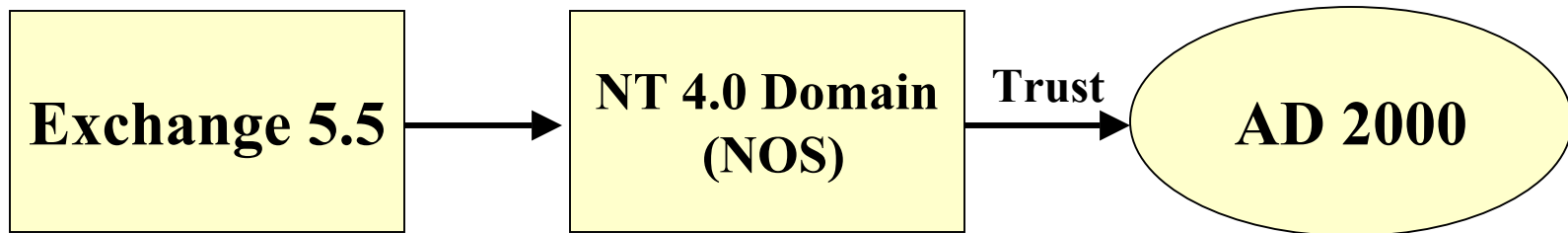


Migration Planning Considerations

- Assign a site lead
- Create public relations plan to educate Commanders, Directors, IMO's and users (Need Buy in from all)
- Develop communities of interest
- Develop an inventory
 - Status of NT Domain Consolidation
 - POCs/Administrators for Each Domain
 - Organizations/Users/Locations/IMO Contacts
 - Desktops (OS's, standard applications)
 - Network Topology and Devices (LAN/BAN/switches, hubs, cabling)
- Identify resources



New Exchange 5.5 Servers



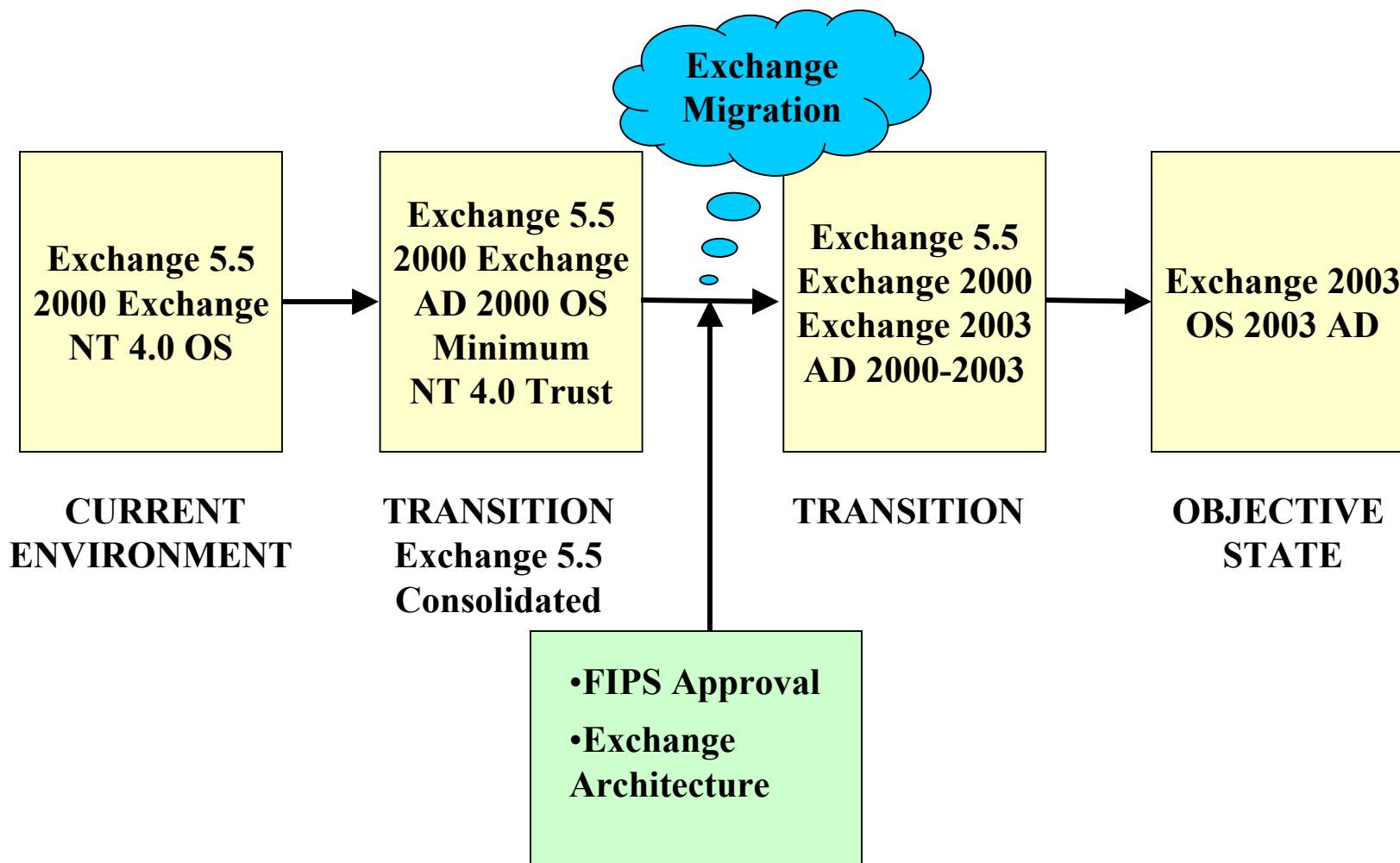
- 2000 OS
- NT 4.0 OS

- Accounts
- Users
- SID History

- Exchange 5.5 and NT 4.0 Domain Consolidation
- New exchange 5.5 servers build on 2000 OS
- All rebuilds of exchange 5.5 on 2000 OS
- Minimum NT 4.0 domain trust (one per installation)



Goal: Exchange 2003





NETCOM / 9th Army Signal Command



Migration Order

- Pick installations that have consolidated NT 4.0 domains and Exchange 5.5 for first migration
- AD 2000 backbone and site Domains installed